1. **TCPA** and Palladium: Sony Inside || kuro5hin.org
The **hypervisor** would provide a complete emulation of a personal computer for **.....** **TPM** signing off by localroger, 07/09/2002 09:54:11 PM EST (4.50 / 4) **...**
www.kuro5hin.org/story/2002/7/9/17842/90350 - 135k - Cached - Similar pages

2. Re: **TPM** & disk crypto
TCPA was focused on a measured boot process. As the system boots, each stage would **...** measure (ie hash into the **TPM**) and launch a **hypervisor**, that is, **...**
www.mail-archive.com/cryptography@metzdowd.com/msg06831.html - 17k - Cached - Similar pages

3. [PDF] Clarifying Misinformation on **TCPA**
File Format: PDF/Adobe Acrobat - View as HTML
"GPL... source alone is worthless without a **TPM** -specific certificate." . The **TCPA** chip performs. all functions without the use of an external certificate. **...**
domino.research.ibm.com/comm/research_projects.nsf/pages/gsal.TCG.html/$FILE/**tcpa**_rebuttal.pdf - Similar pages

4. System and method to lock **TPM** always 'on' using a monitor - Patent **...**
This applies to the **TPM** 322 as well. The boot sequence may follow a Trusted Computing Platform Alliance (**TCPA**) methodology. The Core Root of Trust for **...**
www.freepatentsonline.com/7360253.html - Similar pages

by A Frank - 2008

5. [PDF] Trusted Linux Client
File Format: PDF/Adobe Acrobat - View as HTML
Trusted Computing Platform Alliance (**TCPA**) **.... TPM**. Secure **Hypervisor**. Trusted Platform Module. Trusted. Linux. Client. Legacy. Windows. (on QEMU) **...**
www.acsac.org/2004/workshop/David-Safford.pdf - Similar pages

by D Safford - 2004 - Cited by 3 - Related articles

6. [PDF] Microsoft PowerPoint - TCGIBM_Berlin_Final
File Format: PDF/Adobe Acrobat - View as HTML
•**TPM** can store Integrity Metrics information that is reported to it **....** Secure Virtualization implemented via **hypervisor** on top of platform specific core **...**
ftp.gnumonks.org/pub/congress-talks/.../2_Die%20TCG%20-%20Strategie%20und%

20Konzept%20Dr.%20Michael%20W... - Similar pages

7. 2007 July « root labs rdist
We'll be giving our talk on why a 100% undetectable **hypervisor** is impossible **...** It will be interesting to see how **TCPA** companies respond to the inevitable **...**
rdist.root.org/2007/07/ - 29k - Cached - Similar pages

8. Trusted Code Remote Execution through Trusted Computing and **...**
Trusted Computing Platform Alliance (**TCPA**) in 1999. and it changed to Trusted Computing Group **....** and notify the **TPM** and **hypervisor** to release. resources. **...**
ieeexplore.ieee.org/iel5/4287452/4287453/04287470.pdf?arnumber=4287470 - Similar pages

by L Zhang - 2007 - Cited by 1 - Related articles - All 4 versions

9. Biography
Assisted IBM's PC division with the development of **TCPA** on their platform and developed the **TPM** Linux device drivers [1999-2002]. **...**
www.paramecium.org/~leendert/bio.html - 21k - Cached - Similar pages

10. Design and implementation of a TCG-based integrity measurement **...**
Client integrity is measured using a Trusted Platform Module (**TPM**), **...** We present the sHype **hypervisor** security architecture and examine in detail its **...**
citeseerx.ist.psu.edu/showciting;jsessionid=852585FDC77EF7FFCC06FB332B7319F5?cid=29... - 42k - Cached - Similar pages

Gooooooooooogle ▶
1 2 3 4 5 6 7 8 9 10 **Next**